(19) JAPANESE PATENT OFFICE

(4)

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **01177229 A**

(43) Date of publication of application: **13.07.89**

(51) Int. Cl **H04L 9/02**
G09C 1/00

(21) Application number: **63000959**

(22) Date of filing: **05.01.88**

(71) Applicant: **NEC CORP**

(72) Inventor: **OKAMOTO EIJI**

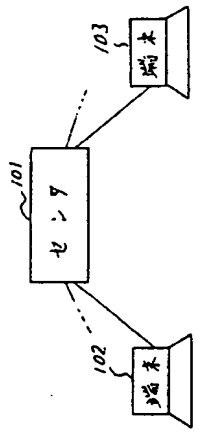
(54) **KEY DISTRIBUTING SYSTEM**

(57) Abstract:

PURPOSE: To prevent an increase in memory by providing a program for cipher between a center and each terminal and making ciphering of data executable if a key is given.

CONSTITUTION: This system is constituted of a center 101 and plural terminals 102, 103.... The user of each terminal sends a ciphered key $EC_1(K)$ obtained by ciphering a key K with the code C_1 held by the user to the center 101 together with the identifying information (ID_1) of the user and the center 101 produces the code C_1. by converting the received information ID_1 by performing prefixed specific conversion and decodes the ciphered key EC_1 (K) so as to obtain the key K. Then the center 101 sends the ciphered key $EC_1(K)$ produced by ciphering the key K by using the code C_1 obtained by performing prefixed specifiic conversion on the identifying information ID_1 to the terminal and, on the terminal side, when the user decodes the received ciphered key $EC_1(K)$ by using the code C_1 held by the user in advance and obtains the key K. Therefore, it is not necessary to increase the number of memories to be used at the center 101.

COPYRIGHT: (C)1989,JPO&Japio



UNEXAMINED PATENT PUBLICATION No. HEI-1-177229
Laid-open date: July 13, 1989

Title of the Invention: Key distribution system

Application No. SHO-63-959
Application date: January 5, 1988

Inventor: Eiji Okamoto
c/o Nippon Electric Co., Ltd.
No. 1, Shiba 5-chome 33, Minato-ku, Tokyo
Applicant: Nippon Electric Co., Ltd.
No. 1, Shiba 5-chome 33, Minato-ku, Tokyo
Agent: Shin Uchihara, patent attorney

SPECIFICATION

Title of the Invention

Key distribtion system

Scope of Claim for a Patent

A key distribution system for distributing a key used for cryptography between a center and a plurality of terminals in a network composed of the center and terminals, characterized in that the user side of the terminal sends both $E_{c1}(K)$ which is obtained by encrypting a key K by using a code C_1 owned by the user and the user's identification information ID_1 to the center, which produces the code C_1 by converting the received ID_1 by a predetermined specific conversion and decrypts the received $E_{c1}(K)$ using the code C_1 thereby to obtain the key K, the center side sends the $E_{c1}(K)$ to the terminal which $E_{c1}(K)$ is obtained by encrypting the key K by using the C_1 obtained by converting the identification information ID_1 of the user with a predetermined specific conversion, and said terminal obtains the key K by decrypting the received $E_{c1}(K)$ using the code C_1 held in advance by the user.

Detailed Description of the Invention

[Industrial Field of Utilization]

The present invention relates to a key distribution system for generating and distributing a key used for cryptography.

[Prior Art]

In a conventional key distribution system of a centralized network, it is widely used that a center holds a key encryption key for each user, and a data encryption key is distributed by being encrypted using this key encryption key. In this case, it is enough for each user to hold only his key encryption key but not the key encryption keys of other users.

[Problem to be Solved by the Invention]

In the system described above, the center is required to have the key encryption keys for all the users and therefore the memory capacity increases with the number of users. Another problem is that each time a new user joins the system, a key encryption key for his/her terminal is required to be added.

[Means for Solving the Problem]

According to this invention, there is provided a key distribution system for distributing a key used for cryptography between a center and a plurality of terminals in a network composed of the center and terminals, the system being so configured that the user side of the terminal sends both $E_{c1}(K)$ which is obtained by encrypting a key K by using a code C_1 owned by him and his identification information ID_1 to the center, which produces the code C_1 by converting the received ID_1 by a predetermined specific conversion and decrypts the received $E_{c1}(K)$ using the code C_1 thereby to obtain the key K, the center side sends the $E_{c1}(K)$ to the terminal which $E_{c1}(K)$ is obtained by encrypting the key K by using the C_1 obtained by converting the identification information ID_1 of the user with a predetermined specific conversion, and said terminal obtains the key K by decrypting the received $E_{c1}(K)$ using the code C_1 held in advance by the user.

[Embodiments]

An embodiment of the present invention will be explained below with reference to the drawings.

Fig. 3 is a diagram showing a configuration of an example of a system to which the invention is applicable.

This system constitutes a network comprising a center 101 and a plurality of terminals 102, 103, and so on. The network is, for example, a computer network or a personal computer communication system. The center and each terminal have an encryption program, and if supplied with a key, can encrypt data or the like. The encryption program is, for example, the Data Encryption Standard established by U.S. DEPARTMENT OF COMMERCE, National Bureau of Standards (hereinafter referred to as DES).

Figs. 1 and 2 are flowcharts showing an embodiment of the invention. Fig. 1(a) shows the flow of encryption process at a terminal, in which a key is generated at the terminal and sent to the center, Fig. 1(b) shows the flow of decryption process in which the key is decrypted at the center, Fig. 2(a) shows the flow of encryption process at the center, in which a key is generated at the center and sent to a given terminal, and Fig. 2(b) shows the flow of decryption process in which the key is decrypted at a terminal. A common digital pattern is set as a key for the transmission side (from a terminal to the center) and the receiving side (from the center to a terminal). Each user is supplied with a key encryption key K_1 from the center or a network management organization. Assuming that the identification information of a user i is ID_i, K_i is given as

$$K_i = f(ID_i)$$

where f is the function known only to the center and the management organization. Also, using, for example, the DES and the confidential code MK, the key encryption key K_i is expressed as,

$$K_i = DES_{MK}(ID_i)$$

where DES_{MK} designates the conversion by DES using MK as a key. Any other confidential function than DES can be used.

In Fig. 1(a), when a key generation program of a terminal is started, WK randomly selected is used as a key (step ①), this WK is encrypted by the key encryption key Ki input by the user to obtain $EWK = E_{Ki}$ (WK) (step ②), and EWK is sent together with the identification information ID_i of

the user to the center (step ③). At the center, a key encryption key K_i is prepared from ID_i (step ④), and a key WK is produced by decrypting EWK (step ⑤) in the manner shown in Fig. 1(b), where $E_K(x)$ and $D_K(x)$ indicate that x is encrypted and decrypted, respectively, with key K. For example, DES can be used in this process.

In Fig. 2(a), the center generates a key WK at random (step ⑥), and based on the identification information ID_i of the transmitting party, generates a key encryption key $K_i = f(ID_i)$ (step ⑦), encrypts the key WK using the key encryption key K_i thereby to obtain $EWK = E_{Ki}(WK)$ (step ⑧), and sends this EWK to the terminal (step ⑨). At the terminal, as shown in Fig. 2(b), upon receipt of the encryption key EWK, decrypts it by the key encryption key K_i input by the user thereby to obtain WK (step ⑩).

In the embodiment described above, the process of encryption and conversion f is carried out by software using DES. Nevertheless, the same process can be carried out by hardware. Also, the address of a terminal but not the user identification information can be used as IDi.

[Effects of the Invention]

As explained in detail above, according to this invention, the memory capacity of the center can be small and a key can be easily distributed as no change is required when a new user joins the system.

Brief Description of the Drawings

Figs. 1 and 2 are flowcharts showing the process flow according to an embodiment of this invention from terminals to the center and from the center to terminals, respectively, and Fig. 3 is a diagram showing a configuration of an example of a system to which the invention is applicable.

101...Center, 102, 103...Terminals

く、端末のアドレスそのものを用いることもできる。

〔発明の効果〕

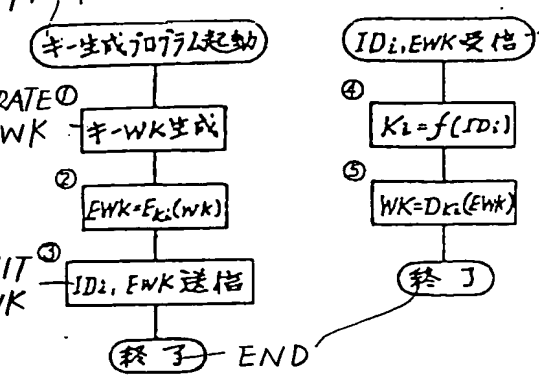
以上詳細に説明したように、本発明を用いればセンタのメモリが少なくて、新規ユーザ加入時にも変更の必要がなく、容易にキーを配送できると言う効果がある。

図面の簡単な説明

第1図および第2図はそれぞれ端末からセンタへ、およびセンタから端末への本発明の一実施例の流れ図、第3図は本発明の適用されるシステムの一例を示す構成図である。

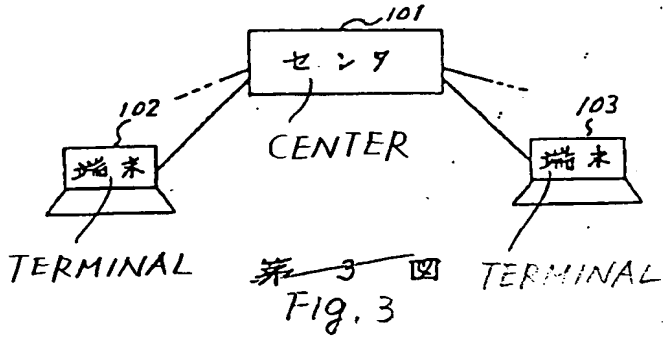
101…センタ、102，103…端末。

代理人　弁理士　内　原　晋

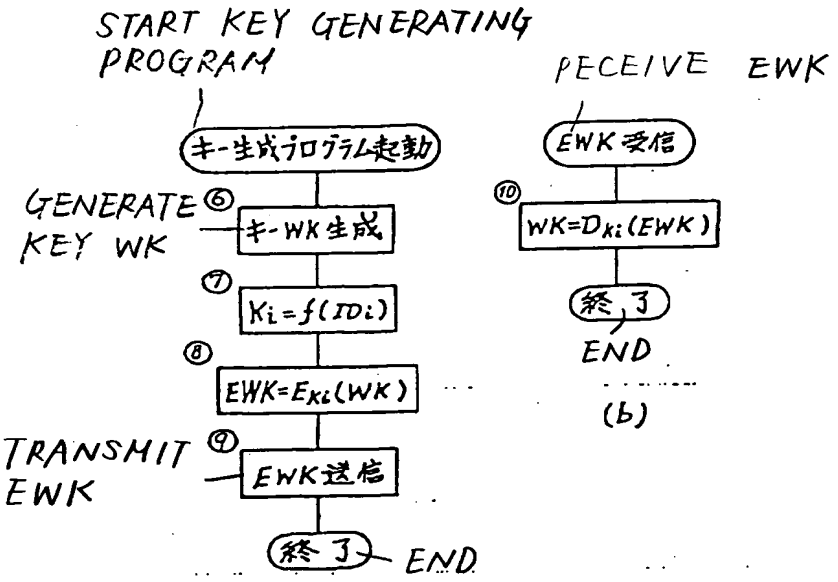


(a)　Fig. 1　(b)

第1図



第3図
Fig. 3



第2図
Fig. 2

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1-177229 (4)

⑤1Int.Cl.⁴　識別記号　庁内整理番号　⑬公開　平成1年(1989)7月13日

H 04 L 9/02　Z-7240-5K
G 09 C 1/00　7368-5B

審査請求　未請求　請求項の数 1　(全3頁)

⑤4発明の名称　キー配送方式

⑳特　願　昭63-959
㉒出　願　昭63(1988)1月5日

㉗発明者　岡本　栄司　東京都港区芝5丁目33番1号　日本電気株式会社内
㉑出願人　日本電気株式会社　東京都港区芝5丁目33番1号
㉔代理人　弁理士　内原　晋

明　細　書

発明の名称

キー配送方式

特許請求の範囲

センタと複数の端末とから成るネットワークにおけるセンタと端末との間で暗号に用いるキーを配送するキー配送方式において、前記端末のユーザ側はキーKをこのユーザが所持するコードC₁で暗号化したEc₁(K)とこのユーザの識別情報ID₁とを共にセンタへ送り、前記センタは受取ったID₁をあらかじめ定められた特定の変換で変換して前記コードC₁を作成し、このC₁で受取った前記Ec₁(K)を復号することにより前記キーKを得て、前記センタ側は前記ユーザの識別情報ID₁をあらかじめ定められた特定の変換で変換したC₁で前記キーKを暗号化したEc₁(K)を前記端末へ送り、この端末は受取ったEc₁(K)を前記ユーザが前もって所持しているコードC₁を用いて復号化することにより前記キーKを得ることを特徴とするキー配送方式。

発明の詳細な説明

(産業上の利用分野)

本発明は暗号に用いるキーを生成し配送するキー配送方式に関する。

(従来の技術)

集中型のネットワークにおける従来のキー配送方式では、センタが各ユーザとの間のキー暗号化キーを全て持っていて、このキー暗号化キーを用いてデータ暗号化キーを暗号化して配送する方式が多用されている。この場合、各ユーザは自分のキー暗号化キーのみを持っていればよく、他のユーザのキー暗号化キーを持っている必要はない。

(発明が解決しようとする問題点)

上述の方式では、センタは各ユーザとの間のキー暗号化キーを全て持つ必要があるので、ユーザ数が増えてくるとメモリが増え、しかも新規ユーザの加入ごとにその端末用キー暗号化キーを追加

する必要があると言う問題点を有している。

〔問題点を解決するための手段〕

本発明のキー配送方式は、センタと複数の端末とから成るネットワークにおけるセンタと端末との間で暗号に用いるキーを配送するキー配送方式において、前記端末のユーザ側はキーKをこのユーザが所持するコードC₁で暗号化したEc₁(K)とこのユーザの識別情報ID₁とを共にセンタへ送り、前記センタは受取ったID₁をあらかじめ定められた特定の変換で変換して前記コードC₁を作成し、このC₁で受取った前記Ec₁(K)を復号することにより前記キーKを得て、前記センタ側は前記ユーザの識別情報ID₁をあらかじめ定められた特定の変換で変換したC₁で前記キーKを暗号化したEc₁(K)を前記端末へ送り、この端末は受取ったEc₁(K)を前記ユーザが前もって所持しているコードC₁を用いて復号化することにより前記キーKを得ることにより構成される。

〔実施例〕

以下、本発明の実施例について図面を参照して説明する。

第3図は本発明が適用されるシステムの一例の構成図である。このシステムはセンタ101と複数の端末102，103，…とから成るネットワークで、例えばコンピュータネットワーク、或いはパソコン通信システムなどである。センタと各端末には暗号用プログラムが設けられていて、キーさえ与えられればデータ等の暗号化が実行できるようになっている。暗号用プログラムは例えばアメリカ商務省標準局が制定したデータ暗号標準（Data Encryption Standard，以下DESと記す）である。

第1図および第2図は本発明の一実施例の流れ図で、第1図（a）が端末でキーを生成してセンタへ送る場合の端末での暗号化を、第1図（b）が同じくセンタでの復号化を、第2図（a）がセンタでキーを生成して端末に送る場合のセンタでの暗号化を、第2図（b）が同じく端末での復号化のフローを示している。キーとしては送信側（端末からセンタへ）と受信側（センタから端末へ）とで共通のディジタル・パターンが設定される。各ユーザはセンタあるいはネットワークの管理機関からキー暗号化キーK₁を与えられている。ここで、ユーザiの識別情報をID₁とすると、K₁は

$$K_1 = f(ID_1)$$

で与えられる。fはセンタと管理機関のみが知っている関数で、例えば前記DESと秘密のコードMKを用いて

$$k_1 = DES_{MK}(ID_1)$$

で与えられる。DES_{MK}はMKをキーとするDESによる変換を示す。なお、DESでなくても秘密の関数ならばよい。

第1図（a）において、端末のキー生成プログラムを起動すると、ランダムに選んだWKをキーとし（ステップ①）、このWKをユーザが入力したキー暗号化キーK₁で暗号化してEWK＝E_{K_1}(WK)を得て（ステップ②）、EWKをユーザの識別情報ID₁と共にセンタへ送る（ステップ③）。センタでは第1図（b）に従って、ID₁からキー暗号化キーK₁を作成し（ステップ④）、EWKを復号化してキーWKを得る（ステップ⑤）。ここで$E_K(x)$および$D_K(x)$はそれぞれxをキーKで暗号化および復号化することを意味する。例えばここでもDESを使える。

第2図（a）ではセンタがランダムにキーWKを生成し（ステップ⑥）、送信者の識別情報ID₁をもとにキー暗号化キーK₁＝f(ID₁)を生成し（ステップ⑦）、これでキーWKを暗号化してEWK＝E_{K_1}(WK)を得て（ステップ⑧）、このEWKを端末に送る（ステップ⑨）。端末では第2図（b）に示すように、暗号化キーEWKを受信すると、ユーザが入力したキー暗号化キーK₁で復号化してWKを得る（ステップ⑩）。

以上の実施例においては、暗号化や変換fにDESを用いてソフトウェアにより処理するものとして説明したが、ハードウェアによって処理してもよい。また、ID₁はユーザの識別情報でな

く、端末のアドレスそのものを用いることもできる。

（発明の効果）

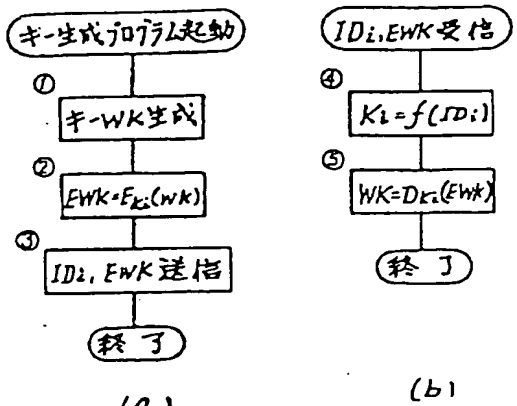
以上詳細に説明したように、本発明を用いればセンタのメモリが少なくて、新規ユーザ加入時にも変更の必要がなく、容易にキーを配送できると言う効果がある。

図面の簡単な説明

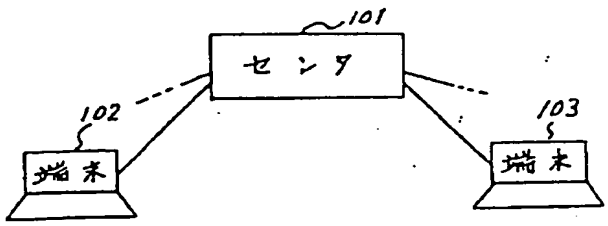
第１図および第２図はそれぞれ端末からセンタへ、およびセンタから端末への本発明の一実施例の流れ図、第３図は本発明の適用されるシステムの一例を示す構成図である。

１０１…センタ、１０２，１０３…端末。

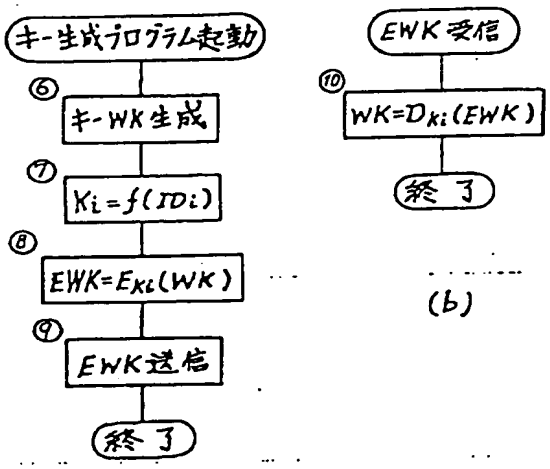
代理人　弁理士　内　原　　晋



第　1　図



第　3　図



第　2　図